PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-068999
(43)Date of publication of application : 03.03.2000

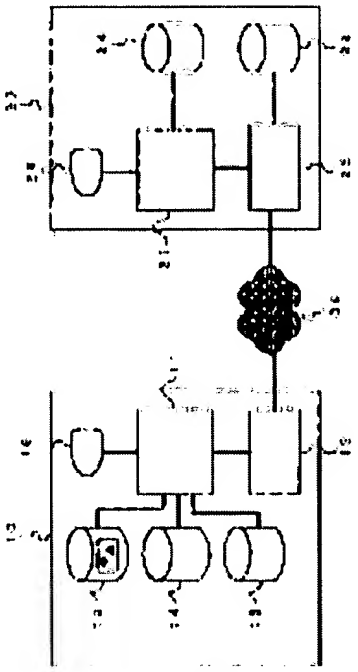
(51)Int.Cl. H04L 9/32
G06F 13/00
G09C 1/00
G09C 5/00
H04L 9/08

(21)Application number : 10-232787
(22)Date of filing : 19.08.1998

(71)Applicant : TOPPAN PRINTING CO LTD
(72)Inventor : OTSUKA KENJI
HAMAYA TAKUMI

(54) SECRECY DATA DISTRIBUTION SYSTEM AND METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To realize distribution of secret data while security of the data is ensured by utilizing the Internet.
SOLUTION: The system is provided with a distribution section 10 consisting of an encoder means 11 that generates distribution data by imbedding secret data and a decoding password in multimedia data by means of an electronic watermark technology in a state of the resulting data that cannot be perceived by people and of an Internet communication means 12 that distributes the distribution data, with a reception section 20 consisting of an Internet communication means 22 that received the distribution data and of a decoder means 21 or the like that extracts the secret data from the distribution data only when a person is identified to be a recipient itself with the decoding password served by the recipient.



LEGAL STATUS

[Date of request for examination] 12.06.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－68999
（P2000－68999A）
(43)公開日　平成12年３月３日(2000.3.3)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ａ	５Ｂ０８９
Ｇ０６Ｆ	13/00	３５４	Ｇ０６Ｆ	13/00	３５４Ｚ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ａ	
	5/00			5/00		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ	

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願平10－232787

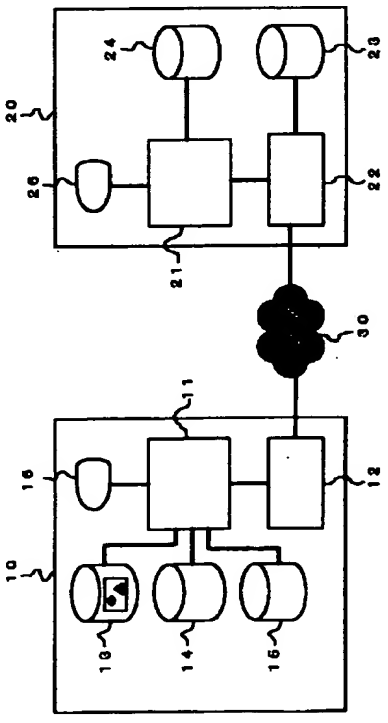
(22)出願日　平成10年８月19日(1998.8.19)

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号
(72)発明者　大塚　健次
東京都台東区台東１丁目５番１号　凸版印刷株式会社内
(72)発明者　浜谷　卓美
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

Ｆターム(参考)　5B089 GB01 JA33 JA40 JB22 JB23 JB24 KB13 KC11 KC47 KC57 KC58
5J104 AA07 AA14 AA16 EA18 KA01 KA04 NA05 PA07

(54)【発明の名称】　機密データ配信システム及び方法

(57)【要約】
【課題】インターネットを利用して機密データを安全かつセキュリティを確保した状態で配信することを実現するために、電子透かし技術を利用することを課題とする。
【解決手段】マルチメディアデータの中に、機密データと解読パスワードとを電子透かし技術により人が知覚できない状態で埋め込むことで配信用データを作るエンコーダ手段１１と、その配信用データを配信するインターネット用通信手段１２などを備える配信部１０と、その配信用データを受け取るインターネット用通信手段２２と、受取人が提供する解読パスワードによって受取人本人であることが確認できたときのみ、その配信用データから機密データを取り出すデコーダ手段２１などを備える受取部２０とを具備する機密データ配信システム。



1

【特許請求の範囲】

【請求項１】インターネットを利用して機密データを配信するシステムであって、

マルチメディアデータの中に、機密データと、受取人本人であることを照合するための解読パスワードとを電子透かし技術を利用して人が知覚できない状態で埋め込むことにより配信用データを作るエンコーダ手段と、その配信用データをインターネットを介して配信するインターネット用通信手段などを備える配信部と、

その配信用データをインターネットを介して受け取るインターネット用通信手段と、受取人が提供する解読パスワードによって受取人本人であることが確認できたときのみ、その配信用データから機密データを取り出すデコーダ手段などを備える受取部と、

を具備することを特徴とする機密データ配信システム。

【請求項２】インターネットを利用して機密データを配信するシステムであって、

機密データを暗号化し、マルチメディアデータの中に、その暗号化された機密データと、受取人本人であることを照合するための解読パスワードとを電子透かし技術を利用して人が知覚できない状態で埋め込むことにより配信用データを作るエンコーダ手段と、その配信用データをインターネットを介して配信するインターネット用通信手段などを備える配信部と、

その配信用データをインターネットを介して受け取るインターネット用通信手段と、受取人が提供する解読パスワードによって受取人本人であることが確認できたときのみ、その配信用データから暗号化された機密データを取り出し、その暗号化された機密データを復号するデコーダ手段などを備える受取部と、

を具備することを特徴とする機密データ配信システム。

【請求項３】インターネットを利用して機密データを配信する方法であって、

配信元或いは第三者は、機密データの配信をする前に、複数の受取人に対し、電子透かし技術によりマルチメディアデータの中に人が知覚できない状態で埋め込まれた機密データを取り出すデコーダ手段と、そのデコーダ手段が受取人本人であることを確認するための解読パスワードを配布し、

配信元は、エンコーダ手段を使用して、そのエンコーダ手段が利用している電子透かし技術によって、マルチメディアデータの中に、受取人に配信する機密データと、受取人の解読パスワードとを人が知覚できない状態で埋め込むことにより配信用データを作った後に、インターネットを利用して、その配信用データを受取人に配信し、

受取人は、インターネットを利用して、その配信用データを受け取った後に、受取人の解読パスワードとデコーダ手段を用いて、その配信用データから機密データを取り出す、

2

ことを特徴とする機密データ配信方法。

【請求項４】インターネットを利用して機密データを配信する方法であって、

配信元或いは第三者は、機密データの配信をする前に、複数の受取人に対し、電子透かし技術によりマルチメディアデータの中に人が知覚できない状態で埋め込まれた暗号化された機密データを取り出し、その暗号化された機密データを復号するデコーダ手段と、そのデコーダ手段が受取人本人であることを確認するための解読パスワードを配布し、

配信元は、エンコーダ手段を使用して、受取人に配信する機密データを暗号化し、そのエンコーダ手段が利用している電子透かし技術によって、マルチメディアデータの中に、その暗号化された機密データと、受取人の解読パスワードとを人が知覚できない状態で埋め込むことにより配信用データを作った後に、インターネットを利用して、その配信用データを受取人に配信し、

受取人は、インターネットを利用して、その配信用データを受け取った後に、受取人の解読パスワードとデコーダ手段を用いて、その配信用データから暗号化された機密データを取り出し、その暗号化された機密データを復号する、

ことを特徴とする機密データ配信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットを利用して配信元から受取人へ安全かつセキュリティを確保した状態で機密データを配信するデータ配信システム及び方法に関する。

【０００２】

【従来の技術】一般的に、機密データを受取人に配信するには、郵便という手段を活用しているが、これは配信元が機密データを郵便封筒の中に入れ封緘を証する割印をすると、郵便という配信インフラが一般的に安全かつセキュリティを確保されたものであるということを、配信元と受取人とが信用しかつ納得し合っているからである。尚、本明細書でいう機密データとは、銀行口座や公共料金の利用明細など、秘匿する必要がある個人のプライバシーに関わる情報のことである。

【０００３】この機密データを郵便という配信インフラに代わってインターネットを用いた電子メールやWWWなどを利用したデータ配信を行おうとした場合、インターネットは郵便とは違い配信インフラ上で第三者が「データ盗聴」、「改ざん」、「なりすまし」などをする危険がつきまとうために、機密データをそのまま配信することは一般に行われていない。

【０００４】従って、機密データをインターネットを利用して配信しようとした場合、郵便物のように郵便封筒の中に機密データを挿入し封緘を証する割印をしたような状態で配信しなければ個人のプライバシを保護するこ

とはできない。また、インターネットの配信経路上で第三者が「データ盗聴」、「改ざん」、「なりすまし」などをすることを防止するような対応をする必要がある。

【０００５】ところで、動画、静止画、音声などのマルチメディアデータに、その冗長性を利用して、他の情報を人が知覚できない状態で埋め込むことができる電子透かし技術と呼ばれるものがある。つまり、電子透かし技術は、動画や静止画に他の情報を不可視の状態で埋め込み、音声には他の情報を聴こえない状態で埋め込む。もちろん、電子透かし技術は、必要なときに、マルチメディアデータに埋め込まれた他の情報を抽出して、人が知覚できるようにすることが可能である。

【０００６】

【発明が解決しようとする課題】そこで、本発明は、インターネットを利用して機密データを安全かつセキュリティを確保した状態で配信することを実現するために、電子透かし技術を利用することを課題とする。

【０００７】

【課題を解決するための手段】本発明において上記の課題を達成するために、まず請求項１の発明では、インターネットを利用して機密データを配信するシステムであって、マルチメディアデータの中に、機密データと、受取人本人であることを照合するための解読パスワードとを電子透かし技術を利用して人が知覚できない状態で埋め込むことにより配信用データを作るエンコーダ手段と、その配信用データをインターネットを介して配信するインターネット用通信手段などを備える配信部と、その配信用データをインターネットを介して受け取るインターネット用通信手段と、受取人が提供する解読パスワードによって受取人本人であることが確認できたときのみ、その配信用データから機密データを取り出すデコーダ手段などを備える受取部と、を具備することを特徴とする機密データ配信システムとしたものである。

【０００８】また請求項２の発明では、インターネットを利用して機密データを配信するシステムであって、機密データを暗号化し、マルチメディアデータの中に、その暗号化された機密データと、受取人本人であることを照合するための解読パスワードとを電子透かし技術を利用して人が知覚できない状態で埋め込むことにより配信用データを作るエンコーダ手段と、その配信用データをインターネットを介して配信するインターネット用通信手段などを備える配信部と、その配信用データをインターネットを介して受け取るインターネット用通信手段と、受取人が提供する解読パスワードによって受取人本人であることが確認できたときのみ、その配信用データから暗号化された機密データを取り出し、その暗号化された機密データを復号するデコーダ手段などを備える受取部と、を具備することを特徴とする機密データ配信システムとしたものである。

【０００９】また請求項３の発明では、インターネットを利用して機密データを配信する方法であって、配信元或いは第三者は、機密データの配信をする前に、複数の受取人に対し、電子透かし技術によりマルチメディアデータの中に人が知覚できない状態で埋め込まれた機密データを取り出すデコーダ手段と、そのデコーダ手段が受取人本人であることを確認するための解読パスワードを配布し、配信元は、エンコーダ手段を使用して、そのエンコーダ手段が利用している電子透かし技術によって、マルチメディアデータの中に、受取人に配信する機密データと、受取人の解読パスワードとを人が知覚できない状態で埋め込むことにより配信用データを作った後に、インターネットを利用して、その配信用データを受取人に配信し、受取人は、インターネットを利用して、その配信用データを受け取った後に、受取人の解読パスワードとデコーダ手段を用いて、その配信用データから機密データを取り出す、ことを特徴とする機密データ配信方法としたものである。

【００１０】また請求項４の発明では、インターネットを利用して機密データを配信する方法であって、配信元或いは第三者は、機密データの配信をする前に、複数の受取人に対し、電子透かし技術によりマルチメディアデータの中に人が知覚できない状態で埋め込まれた暗号化された機密データを取り出し、その暗号化された機密データを復号するデコーダ手段と、そのデコーダ手段が受取人本人であることを確認するための解読パスワードを配布し、配信元は、エンコーダ手段を使用して、受取人に配信する機密データを暗号化し、そのエンコーダ手段が利用している電子透かし技術によって、マルチメディアデータの中に、その暗号化された機密データと、受取人の解読パスワードとを人が知覚できない状態で埋め込むことにより配信用データを作った後に、インターネットを利用して、その配信用データを受取人に配信し、受取人は、インターネットを利用して、その配信用データを受け取った後に、受取人の解読パスワードとデコーダ手段を用いて、その配信用データから暗号化された機密データを取り出し、その暗号化された機密データを復号することを特徴とする機密データ配信方法としたものである。

【００１１】

【発明の実施の形態】以下で、本発明の実施の形態を、図１～３を用いて説明する。

【００１２】本発明は、配信元が、電子透かし技術を用いて、マルチメディアデータの中に機密データを人が知覚できない状態で埋め込んだ後にそのマルチメディアデータをインターネットで受取人に送り、受取人本人のみがマルチメディアデータから機密データを取り出して知覚できるようにするシステムと方法である。本明細書では、説明を簡便にするために、電子透かし技術を用いてマルチメディアデータの中に機密データを人が知覚できない状態で埋め込むことを、マルチメディアデータの中

に機密データを隠蔽すると表現することにする。

【００１３】本発明システムは、図１に見られるように、インターネット３０を介して配信用データを送る配信部１０と、同じくインターネット３０を介して配信用データを受け取る受取部２０からなる。

【００１４】配信部１０おいて、配信元は、エンコーダ手段１１を利用して、マルチメディアデータ保管手段１３に保管されているマルチメディアデータから所望のマルチメディアデータ、機密データ保管手段１４に保管されている機密データから所望の機密データ、解読パスワード保管手段１５に保管されている解読パスワードから所望の解読パスワードを選び、マルチメディアデータの中に機密データと解読パスワードを隠蔽して配信用データを作る。その後、配信元は、インターネット用通信手段１２によってインターネット３０を介して、マルチメディアデータにの中に隠蔽された解読パスワードを持つ受取人にその配信用データを送る。

【００１５】受取部２０において、受取人は、インターネット用通信手段２２によってインターネット３０を介して、配信元から送られてきた配信用データを受け取り、受取データ保管手段２３に保管する。受取人は、デコーダ手段２１を用いて、受取データ保管手段２３に保管されている配信用データの中から所望の配信データを選び、その配信用データから機密データを取り出すのであるが、デコーダ手段２１は、次のような処理を行う。すなわち、デコーダ手段２１は、受取人に受取人の解読パスワードを提供することを要求し、受取人の解読パスワードと配信用データの中にある解読パスワードとを照合する。その結果、２つの解読パスワードが一致したときのみ、デコーダ手段２１は、配信用データから機密データを取り出し、受取人に知覚できるように表現する。最後に、受取人が機密データを知覚した後、デコーダ手段２１は、機密データを、機密データ保管手段２４に保管するか、或いは削除する。

【００１６】尚、解読パスワードとデコーダ手段２１とは、機密データの配信をする前に、受取人に配布してあるものとする。配布する主体は、配信元であっても良いし、公的機関などの第三者であっても良い。

【００１７】インターネット用通信手段１２及び２２は、インターネットとの接続機能があるコンピュータ或いはコンピュータネットワークである。エンコーダ手段１１は、ハードウェアであっても良いし、インターネット用通信手段１２を構成するコンピュータ上で動作するソフトウェアであっても良い。同様に、デコーダ手段２１は、ハードウェアであっても良いし、インターネット用通信手段２２を構成するコンピュータ上で動作するソフトウェアであっても良い。マルチメディアデータ保管手段１３、機密データ保管手段１４、解読パスワード保管手段１５は、データベースであっても良いし、或いはインターネット通信用手段１２を構成するコンピュータが利用しているファイルシステムであっても良い。同じく、受取データ保管手段２３、機密データ保管手段２４は、データベースであっても良いし、或いはインターネット通信用手段２２を構成するコンピュータが利用しているファイルシステムであっても良い。

【００１８】配信元が、エンコーダ手段１１を利用して、マルチメディアデータの中に、機密データと解読パスワードを隠蔽する処理の１例を、図２のフローチャートに従って説明する。

【００１９】ＳＴＥＰ１において、表示手段１６にマルチメディアデータの指定画面を表示し、マルチメディアデータ保管手段１３に保管されているマルチメディアデータの中から、所望のマルチメディアデータを指定して選ぶ。表示手段１６の具体例としては、ＣＲＴ（Ｃａｔｈｏｄｅ－Ｒａｙ　Ｔｕｂｅ）ディスプレイ、或いは液晶ディスプレイが挙げられる。

【００２０】ＳＴＥＰ２において、表示手段１６に機密データ及び解読パスワード指定画面を表示し、機密データ保管手段１４に保管されている機密データの中から受取人に配信したい所望の機密データを指定して選ぶ。次に、解読パスワード保管手段１５に保管されている解読パスワードの中から所望の解読パスワードを指定する。

【００２１】ＳＴＥＰ３において、ＳＴＥＰ２で指定した機密データと解読パスワードを、マルチメディアデータの中に隠蔽する。

【００２２】ＳＴＥＰ４において、機密データと解読パスワードを隠蔽したマルチメディアデータを配信用データとして、インターネット用通信手段１２に渡す。

【００２３】受取人が、デコーダ手段２１を利用して、配信用データから、機密データを取り出す処理の１例を、図３のフローチャートに従って説明する。

【００２４】ＳＴＥＰ１において、表示手段２６に配信用データの指定画面を表示し、受取データ保管手段２３に保管されている配信用データの中から、所望の配信用データを指定して選ぶ。表示手段２６の具体例としては、ＣＲＴ（Ｃａｔｈｏｄｅ－Ｒａｙ　Ｔｕｂｅ）ディスプレイ、或いは液晶ディスプレイが挙げられる。

【００２５】ＳＴＥＰ２において、表示手段２６に解読パスワード入力画面を表示させ、受取人のパスワードを入力する。

【００２６】ＳＴＥＰ３において、デコーダ手段２１は、受取人が入力した解読パスワードと配信用データの中にある解読パスワードとが一致するかを確認する。一致しなければ、ＳＴＥＰ２に戻る。この際に、解読パスワードを例えば３回以上間違った場合、デコーダ手段２１は配信用データを受取データ保管手段２３から削除することによって、受取人以外がデコーダ手段２１を不正使用した場合の保護対策を追加しても良い。他方、一致すれば、ＳＴＥＰ４に進む。

【００２７】ＳＴＥＰ４において、デコーダ手段２１

は、配信用データから機密データを取り出す。

【００２８】ＳＴＥＰ５において、デコーダ手段２１は、機密データを受取人に知覚できるように表現する。

【００２９】更に、安全性とセキュリティを強化するために、電子透かし技術とは異なる暗号技術を併用しても良い。例えば、エンコーダ手段１１は、機密データを暗号化した後に、その暗号化された機密データをマルチメディアデータの中に隠蔽して配信用データを作成し、そして、デコーダ手段２１は、配信用データから暗号化された機密データを取り出した後にその暗号化された機密データを復号するようにしても良い。

【００３０】

【発明の効果】本発明は、以下のような効果がある。まず、マルチメディアデータの中に機密データを隠蔽して配信しているので、配信元から受取人に届くまでの間に第三者が配信用データを盗聴しても、マルチメディアデータが配信されていると思い込むだけで、その中に機密データが隠されているとは思いもよらない。また、仮にマルチメディアデータに機密データが隠蔽されていることが漏れたとしても、デコーダ手段を入手し、しかも解読パスワードが分からなければ、機密データを取り出すことはできない。

【図面の簡単な説明】

【図１】本発明の機密データ配信システムの構成を説明する図である。

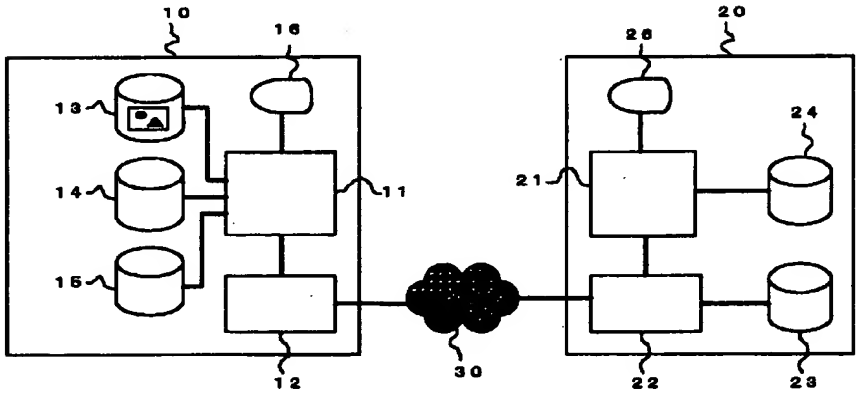
【図２】配信用データを作成する処理を説明するフローチャートである。

【図３】配信用データから機密データを取り出す処理を説明するフローチャートである。

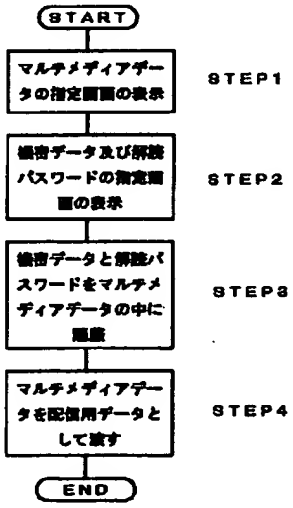
【符号の説明】

１０…配信部
１１…エンコーダ手段
１２…インターネット用通信手段
１３…マルチメディアデータ保管手段
１４…機密データ保管手段
１５…解読パスワード保管手段
１６…表示手段
２０…受取部
２１…デコーダ手段
２２…インターネット用通信手段
２３…受取データ保管手段
２４…機密データ保管手段
２６…表示手段
３０…インターネット

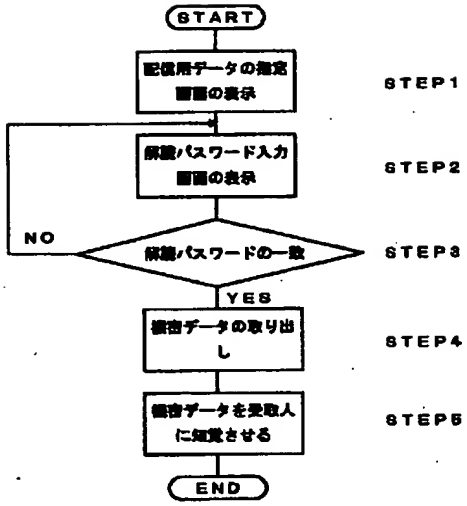
【図１】



【図２】



【図３】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード'(参考)
		Ｈ０４Ｌ　9/00	６０１Ｅ	